International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-4, November 2019

Wireless Technologies and Process Automation

Nasr Rashid, Osama I. Elhamrawy

Abstract: ***Prerequisites for the field communications networks in the process industries include effective support for hybrid traffic, durability, availability, reliability, security, and scalability in a harsh industrial environment. Moreover, the establishment of such a network on a license-free scale raises worries regarding its security, safety, functioning and service quality (QoS). Quality of Service relates to the management of network resources and the provision of services required by the application by controlling delay, jitter, packet loss rate and bandwidth. To develop an industrial-strength wireless network that can handle stringent process automation requirements, impose restrictions on network design that includes hardware and software components used. To achieve the quality of service required, a broad view of systems must be seen as the overall performance of network-based applications based on the operation, interaction and collaboration of individual components. To achieve the perceived network, various problems are dealt with. As part of this research, three specific issues were addressed: time synchronization problem in distributed systems, closed-loop control on a resource-constrained wireless network, and transmission power monitoring (TPC) in wireless field nodes. They address the problem of limited resources available in distributed field nodes with a view to maximizing the use of available resources. This will be explained in detail later. Recent developments in wireless communications technologies creating new opportunities for wireless communication to field equipment in industries such as gas and oil, bulk water distribution and chemical processing. Wireless communications can help the above industries improve factory knowledge by getting complementary, measurements of operations and devices when wired communication is not allowed. The operational field communications network requirements include active support for hybrid traffic, durability, reliability, safety, and scalability in the industrial environment of harsh. Moreover, the establishment of such a network on a scale that does not carry any license raises worries regarding its security, safety, functioning and governance.***

Keywords: Wireless Technologies, Process Automation, Condition Monitoring.

I. INTRODUCTION

The prerequisites of a field communication networks in process industries include real time support for hybrid traffic, durability, availability, reliability, security, and scalability in a harsh industrial environment. Moreover, to establishment such a network on license-exempt band raises worries regarding its safety, security, functioning and Quality of Service (QoS)[1,2]. QoS is about managing network resources and offering services which are required by application by means of controlling delay, jitter, packet loss rate and bandwidth. To develop an industrial strength wireless network which can address these stringent process automation requirements imposes restrictions on the network design which incorporates the hardware and software components used. [2]To achieve the required QoS, a wider view of systems has to be considered as the overall performance of network based applications will rely on operation of individual components, their interaction and cooperation. To achieve the envisioned network, various problems are to be dealt with. As part of this research, three specific issues have been addressed; namely, time synchronization issue in distributed systems, closed-loop control over a resource-constraint wireless networks, and Transmission Power Control (TPC) in wireless field nodes.[2,3] They address the issue linked to limited resources available in distributed field nodes with the aim of maximizing the use of available resources. They will be explained in detail later.[4]

II. OPPORTUNITIES FOR WIRELESS COMMUNICATION IN PROCESS AUTOMATION

Fig. 1 presents an overview of sensor network applications as found in process industries. The applications are divided into two divisions: monitoring and tracking, based on application requirements.[5] The monitoring domain refers to applications which rely on industrial measurements for the purpose of regulatory compliance, equipment and infrastructure condition monitoring, process control and on-site safety. These activities may require wider collaboration between distributed sensors. The other division is tracking and refers to locating of individuals or equipment. In this case the proximity of these objects in space is of concern and the data from individual nodes is sufficient to draw conclusions. Tracking is important for the purpose of supply chain optimization and emergency response management.[2,4]

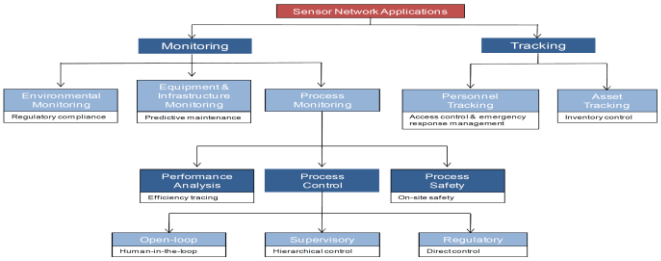

Fig. 1 Overview of sensors network applications in industry

Manuscript published on November 30, 2019.
* Correspondence Author
Nasr Rashid*, Assistant Professor in the Department of Electrical Engineering, College of Engineering, Jouf University, Sakaka, Saudi Arabia
Osama I. EL-Hamrawy, Assistant Professor in the Department of Electrical Engineering, College of Engineering, Jouf University, Sakaka, Saudi Arabia.

Table I presents non-exhaustive list of applications found in process automation based on the overview of sensor networks outlined in Fig. 1. Table I shows that wireless communication enables better utilization of assets, enhances workforce productivity, assists compliance with regulations, improves on-site safety, and allows connections to locations which were either unfeasible or uneconomical to reach in the past.[6] According to Drathen (2009) the use of wireless technology and the internet will become significant for process automation in future to provide up-to-date knowledge of on-going activities and effective knowledge management.[7] Other commentators suggest that wireless communications will improve the monitoring and visibility of processes and equipment and achieve higher yields and better quality at lower costs Process industry automation activities are classified by ISA and NAMUR as related to safety, control or monitoring applications. Due to the criticality associated with the safety data, and data linked to critical-control applications, wired solutions are currently considered the best available methods within these domains. [8] However, as shown in Table I wireless communications are being used in process automation, especially when the update-rate is moderate and the application is non-critical. [2] The current focus is on monitoring applications. Use of wireless communications in feedback control loop is developing considerably more slowly for reasons that will be explored in later section.[9]

Table-I**:**Applications of wireless communications in industry**.**

Collection of diagnostic data from 4-20 mA process instruments:
Conventional 4-20mA current loop instruments are progressively becoming equipped with HART protocol that provides diagnostics data for condition supervision and maintenance.
Tracking and tracing:
Radio frequency identification tagging (RFID) uses an electronic barcode that can be read remotely. RFIDs are in routine use in supply series operations for stocking tracking and also enable tracking and tracing of personnel and equipment, with benefit for safety.
Difficult measurement sites:
Wireless communications enable access to measurement from remote or inaccessible sites where wired connectivity is infeasible, costly or too bulky or heavy. Wireless communications eliminate cables, and occupies less space.
Equipment condition monitoring and predictive maintenance:
Mechanical fails of equipment such as motors and drives are amongst the most common causes of stoppage of production.
Field rounds:
Measurements in process plant are often documented manually by engineers in the field. Examples include corrosion monitoring on critical areas of pipelines or vessels, temperature, ball valve position and level monitoring in tank farms. WSNs can collect this data automatically and eliminate or speed up manual cyclic patrol checks, for instance, they enable collection of data while an operator drives past the equipment.
Safety and environmental monitoring:
Applications related to safety include gas and fire detection and elimination of spills to avoid safety violations. Novel application is the monitoring of eye wash and safety showers to mobilize an emergency response.
Short-term deployments and new sites:
Short-term measurements can use wireless communication, e.g. in equipment monitoring where one costly sensor is installed at different locations in site over time interval. The alternative is to store the data within the instrument and download it at the end of the monitoring interval. On new sites, or extensions of existing sites, the cost effectiveness of wireless installation and the reduction of cable runs may make wireless communications attractive.
Distributed and remote facilities
Wireless communication enables remote operation of facilities. These include: pipelines, loading piers, tank farms, production platforms and wellheads.

III. AUTOMATION PYRAMID AND USAGE CLASSES

The need for automation is necessary for many applications belonging to both industrial and non-industrial domains. Fig. 2 shows the hierarchical view of these automation domains. [2,10]However, the requirements differ between each domain. Industrial automation has more stringent requirement due to the criticality of the operations involved. Two forms of automation used in the industry are factory automation and process automation. [11]Factory automation is related to manufacturing and its operations are confined within production cell, such as the operation of robot arm. Process automation on the other hand involves automation of process like that of distillation column, as found in an oil refinery.[12] There are different sets of requirements for both and the requirements differ in many ways like availability and coverage requirements. As mentioned earlier, process automation refers to the set of technologies working together to attain superior operational performance of processes, machines and systems without significant human intervention. Therefore, it involves synchronization of devices, technologies and the overall integration of machines into self-governing system. It requires bringing technologies together and makes them operate autonomously.[13]

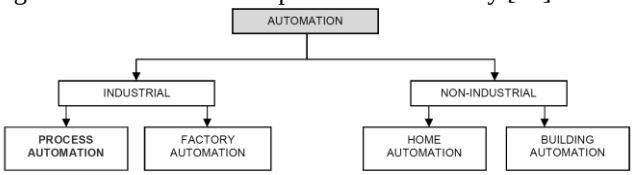

Fig. 2 Hierarchical view of automation classes

A. Automation Pyramid

The industrial automation systems comprise various systems and devices responsible for variety of functions related to instrumentation, control, supervision and operational management. Fig. 3 shows the hierarchical structure of an industrial automation system based on ISA-95 functional hierarchy from ISA-95 Part. [14] The different layers in the automation pyramid represent different sets of application requirements linked to their corresponding activities.

There are five distinct layers of functional hierarchy in the automation pyramid.[15] At the bottom of the pyramid is Layer 0, which can also be referred to as sensor and actuator layer. This layer is closest to the physical process. It is at this layer that the data is collected from field devices like sensors, and sent to the higher layers for analysis and decision making. Similarly, actuators also implement the commands issued by controllers at this level. Level provides services to Level which is responsible for regulatory control. It is at this layer where Programmable Logic Controllers (PLCs) reside. The PLCs interact with field devices and perform real-time control.[16]The next layer is Level which is the supervisory control and operations layer. This layer is responsible for operations of the automatic control layer. This layer sets out the control parameters for the controllers. The regulatory layer looks after the control loops and also the equipment. SCADA systems are used for monitoring and controlling of devices like PLCs.[17] Level on the other hand deals with operational and management related activities such as detailed production scheduling, managing resources, scheduling maintenance and dispatching production. Manufacturing Execution Systems (MES) are found at this layer.[18,19] This layer is related to enterprise management and deals with the commercial aspects of the business. The tasks involved are linked to production targets, plant production scheduling and overall management. High level planning systems such as Enterprise Resource Planning (ERP) systems are used at this level which relies on the services of MESs. [13] The focus of this research is on Levels 0 and 1 that use sensors to collect process data which is further used for various tasks such as calculation of control actions. The arrow heads on the left side of Fig. 3 show that, for wired connections, the amount of cabling increases lower in the hierarchy and the requirements for safety, reliability, transmission frequency and real-time communications also increase. The trend is that at the bottom of the pyramid, the timeliness of information becomes vital as it is directly linked to the operation of equipment or the performance of a process. Reliability of a communication network used at this level is also very critical and is further linked to safety[20, 21]. Moreover, as the numbers of components in the bottom layer is high they require more connections. Wireless connections have the benefit of reducing the amount of cabling. Furthermore, the operating conditions in a process industry are also often harsh compared to the ones present at the higher layers. On the other hand, the volume of data at the bottom of the pyramid is less as it is related to process values whereas the volume of data found at higher layers is high .[22]It is due to these requirements that various network types are used concurrently in industrial automation. The 4-20 mA control loop, HART protocol and fieldbus are examples of technologies designed to connect sensors, actuators and controllers. At the higher levels the wide area network or local area network technologies can be used which can be IP-based networks, such as Ethernet or wireless LAN (Wi-Fi). [21]The bottom two layers are of interest to this research and this is where wireless technology can have significant impact on the process automation. It is based on the requirements of this level that the currently available wireless solutions will be evaluated. All of the higher layers have less stringent application requirement, and the commercially available solutions are already addressing their needs. [2]

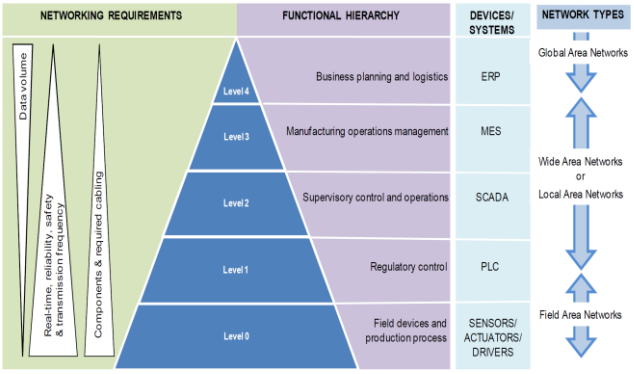

Fig. 3. The automation pyramid

B. Usage Classes

In process automation various applications exist and they have different requirements and levels of tolerance towards timelines of message delivery. The ISA100 working group has identified six different classes within the process automation domain which are classified based on timing restrictions and the criticality of the information. [23]They are shown in Table II. At the field network level, the applications belonging to monitoring domain and open loop control have less stringent requirements and wireless networks are currently being used in such deployments. [2]

Table-II: Classification of process automation applications based on ISA100 workgroup and specifications of NAMUR.

Category	Classification	Description
Safety	**ISAClass0:** Emergency action **NAMUR Class A:**Functional Safety	Always critical
Control	**ISAClass1:** Closed loop regulatory control **NAMUR Class B:** Process/ Management Control	Often critical
	ISAClass2: Closed loop supervisory control **NAMUR Class B:** Process/ Management Control	Usually non-critical
	ISAClass3: Open loop control **NAMUR Class B:** Process/ Management Control	Human in the loop
Monitoring	**ISAClass4:** Alerting **NAMUR Class C:** Display/ Monitoring	Short-term operational consequence
	ISAClass5: Logging and down-loading/ uploading **NAMUR Class C:** Display/ Monitoring	No immediate operational consequence

However, the higher two classes have more complexity involved. The guarantees on the network availability and its stability are important. In case of the safety application, wired networks are currently considered as the most reliable options. In the case of Class 1 which involves closed-loop regulatory control, the requirements are further linked to the process which needs to be controlled. The parameters which are linked to the dynamics of the physical process such as, its response time and dead time, specify the sampling rates for the sensors and controller. Based on the discussion above and the requirements mentioned earlier, the ISA usage classes can be represented on a 3-dimensional axis as shown in Fig. 4.

[2]The three axes here represent update rate, availability and reliability in general. The mapping represents a general overview of relative standing of each application.

The terminologies used in Fig. 4 are highlighted in Table III. Within this graph, closed loop regulatory control as defined by the ISA group can further be subdivided into fast and slow loop control.[2] It is to signify that it is linked to process dynamics and the update rate (i.e. sampling rate) required will vary from process to process[13]. It also highlights that some processes which may have slow process dynamics may be eligible for control over a wireless network. For the other loops which require fast update rate, they mandate the need for certain bandwidth capacity, network topology, and channel access mechanism. If a network cannot provide these features then running a control application over a wireless network may not be an option. From here onwards fast loop control will refer to control which requires sampling period of 1s or below. [13]Table-III. The terminology used in the application requirements for each illustration of the usage category

Reliability: is the percentage of sensor data which reaches its destination, normally the gateway.
Stability: is the percentage of transmitted data successfully delivered to destination. It takes into account retransmissions
Availability: The number of packets that arrive within a predetermined period of time.
Update Rate: is the rate of the number of transmissions per unit of time

Additionally, safety applications are further split into process safety and machine safety based on the requirement of update rate. This detailed layout of applications presented in Fig. 4 signifies that with relaxed update rate requirement, advance methods can be deployed to achieve the requirement of availability and reliability. Fig. 3 also highlights that there may not be one solution for all applications. In some cases, the design of a communication network to address a particular requirement like update rate, availability and reliability may dominate the entire network design. These governing design principles will impose restrictions on networking architecture, routing and redundancy. As a result, the network may not be optimal for use for other classes of applications, other than the intended one.[2, 24]

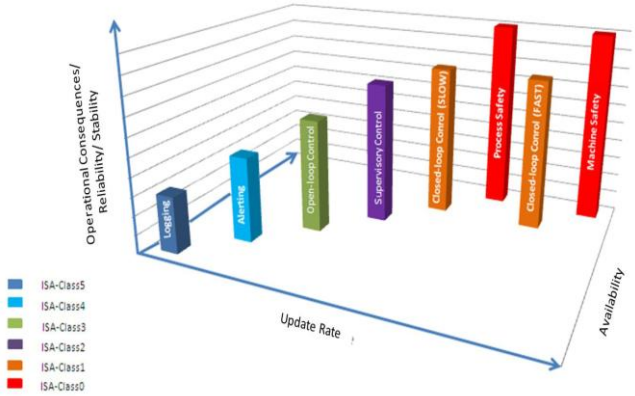

Fig. 4. Application requirements for each usage category.

IV. COMPARISON OF COMMERCIAL WIRELESS COMMUNICATIONS TECHNOLOGIES

Fig. 5 presents the seven-layer OSI model and maps the scope of IEEE 802 standards to the model.[2] It highlights that the lower two-layers, the PHY and MAC layers are within the scope of the IEEE 802 suite of standards. MAC is a sub layer of data link layer. PHY is the lowest layer of the OSI model, also known as Layer 1, and deals with transmission of raw bits over a medium. MAC layer on the other hand is responsible for managing and coordinating access to shared medium. Furthermore, the protocol stack of each of the aforementioned technologies is shown in the Fig. 5 for comparison.[10]

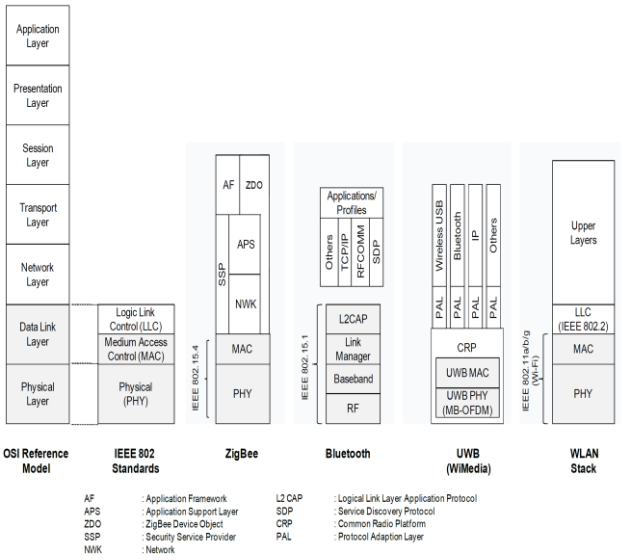

Fig. 5. IEEE 802 standards relate to WPAN and WLAN protocol architectureFrom the figure it can be seen that the lowest two layers of ZigBee, Bluetooth and WLAN stack have associated IEEE 802.xx standard. The ZigBee protocol stack builds upon the IEEE 802.15.4 standard, and the upper layers are specified by ZigBee Alliance. In case of Bluetooth stack they are specified by Bluetooth SIG. The WiMedia UWB specification is formulated by WiMedia Alliance.[16] The Common Radio Platform (CRP), which includes PHY and MAC, is part of the specification and the Protocol Adaption Layer (PAL), and

provides mean to bridge the MAC sublayer to the protocols at upper layers. In the case of WLAN stack, the lower layers are certified by Wi-Fi Alliance. Above these layers protocols such as TCP/IP can operate. Table IV shows typical applications and technical specifications for the commercially available communication protocols in Wireless Personal Area Network (WPAN) and Wireless Local Area Network (WLAN). [2] The frequency bands, bandwidth, modulation, spreading and transmission power in the physical layer are specified by the relevant IEEE 802 family of standards. Distance and data rates are dependent on these parameters. UWB has the fastest supported data rate within a confined radius of less than 10 meters, whereas, Wi-Fi in general supports fast data rate over longer distance. [19] The term spreading refers to spread spectrum, where the signal occupies a bandwidth in excess of the minimum necessary to transmit the information.

It is accomplished by means of a code which is independent of source data. Its ability to resist jamming and interference are amongst the main reasons for the use of spread spectrum techniques.

The widely used techniques for spread spectrum include Frequency Hopping Spread Spectrum (FHSS) and Direct Sequence Spread Spectrum (DSSS).[16] In case of FHSS, the available bandwidth can be divided into a number of channels, each with a slightly different carrier frequency so that messages can be sent in different channels as needed to avoid interference. Therefore, instead of transmitting at one frequency the spread spectrum system switches rapidly from one frequency to the other. The selection of the next frequency in the sequence is random and makes it robust against narrow band jamming. The idea of spread spectrum originated with actress Hedy Lamarr and collaborator George Antheil who patented the idea and a method for implementation in 1942 to avoid jamming of radio-guided torpedoes.[12]

Table-IV: Comparison of short-range wireless communication technologies

	UWB	Bluetooth	ZigBee	Wi-Fi
Frequency band(s)	3.1-10.6 GHz [1], 4.8-6 GHz [2]	2.4 GHz	868 MHz[3], 915 MHz[4], 2.4 GHz*	SubGHz, 2.4 GHz, 5 GHz
Bandwidth	528 MHz [9]	1 MHz	0.6 MHz, 1.2 MHz, 2.0 MHz	a: 16.25 MHz, b: 22 MHz g: 16.25-22 MHz
Raw data rate	480 Mbps[9]	1, 2, 3 Mbps[6]	250 kbps[7]	0.1–54 Mbps
Nominal transmission power	−41.3 dBm/MHz [8] (39.1 µW / band) [9]	0 – 10 dBm	(−25) – 0 (dBm)	15 – 20 dBm
Spreading	DS-UWB, MB-OFDM	FHSS	DSSS	DSSS, OFDM
Basic cell [Extensions]	Peer-to-peer [9], piconet [5] [Child piconet]	Piconet [Scatternet]	Star, [Tree, mesh]	BSS [ESS]
Node enumeration time	Protocol dependent	< 10 s	30 ms (typical)	< 3 s
Medium access	CSMA/CA (TDMA optional)	TDD (master slave polling)	CSMA/CA	CSMA/CA (TDMA optional)
Supported number of nodes	Protocol dependent	8 (7 active slaves)	65,535	2007 (Structured BSS)
Data protection	32-bit CRC	16-bit CRC	16-bit CRC	32-bit CRC
Encryption	AES block cipher	Stream cipher	AES block cipher	AES block cipher [10]
Power consumption	Low	Low	Very low	High
Nominal range (m)	1-10	1-100	10-30	100
Associated IEEE standard	-	IEEE 802.15.1	IEEE 802.15.4	IEEE 802.11a/b/g
Organization(s)	UWB Forum and WiMedia Alliance	Bluetooth SIG	ZigBee Alliance	Wi-Fi Alliance

* Global 1,4 America 2,3 Europe 5 DS-UWB (UWB Forum) 6 v2.1 7 2.4GHz (IEEE 802.15.4-2003) 8 FCC defined spectral density 9 MB-OFDM (WiMedia) 10WPA2 The use of a spread spectrum requires a synchronized decoder in the receiver as well as an encoder in the sending device. Bluetooth adopts this method of spreading. In case of DSSS, the frequency of the carrier is constant. The information signal in this case is multiplied with pseudo random spreading code. Each bit in the spreading code is alled a chip. [25] This spreading code has a higher chip rate and results in a wideband signal. ZigBee and Wi-Fi uses DSSS which offers resistant against interference and gives the ability to share a single channel among multiple users. The MAC protocol enables multiple devices to transmit and share the capacity of the same physical space. ZigBee and Wi-Fi MAC are based on CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) which means that each node monitors the transmissions of other nodes to determine whether the channel is busy or idle. A consequence of this contention-based channel access is that the transmission waiting times are random, in contrast to Time Division Multiple Access (TDMA). [25]In TDMA systems the time axis is divided into time slots and the nodes are assigned times to transmit. TDMA provides deterministic communication as the channel access is contention-free. In terms of network topology, ZigBee offers the most flexibility compared to others. Bluetooth and UWB (DS-UWB) is restrictive as the basic unit of operation is a piconet. The data protection method employed by the technologies presented in Table IV is Cyclic Redundancy Check (CRC) and is part of data link layer. In this method of verifying the integrity of data during transfers, a CRC word (also called checksum) is appended at the end of each data packet. It is an extension of the parity bit method.[21] CRC is generated by dividing the message bits by a fixed binary string referred to as generator polynomial and the remainder is the checksum. By carefully selecting amongst the available standardized polynomials, most of the errors can be detected which occurred during transmission. The use of 16-bits CRC means that the checksum size is 16 bits and the algorithm is able to detect error burst lengths of up to 16 bits. Error burst length refers to number of bits between and including erroneous bits. ZigBee and Bluetooth use 16 bit CRC, whereas, UWB and Wi-Fi uses 32 bit CRC[5]. In terms of message encryption, ZigBee, UWB and Wi-Fi support AES block ciphers, whereas, Bluetooth uses a stream cipher called E0. Block ciphers divide the input stream of bits into discrete sections called blocks and encrypts them.[3]

V. COMPARISON OF INDUSTRIAL STANDARDS

Fig. 5 represents the seven-layer OSI model and maps it to WirelessHART, ISA100.11a and WIA-PA stack architecture. Standard WSN stack implementations consist of five-layers as opposed to seven-layer reference OSI model. The physical layer of all of them is based on IEEE 802.15.4 radio.

WirelessHART and ISA100.11a further define the four higher layers. In the case of WIA-PA the above three layers are defined by the standard. A discussion on each row is provided underneath.

A. Origins

ZigBee PRO is a variant of ZigBee with enhancements for high security and message routing. One of its main uses is for building automation. WirelessHART extended the existing HART protocol, for getting HART information from existing field devices. HART is a bi-directional communication protocol which transmits digital information in addition to process data, for instance remote diagnostics for a field device. It is widely used in the process industries. ISA100.11a and WIA-PA are new protocols created specifically for wireless process automation.[21]

B. Physical Layer

The physical layer is the same in each case when operated in 2.4GHz ISM band using DSSS and O-QPSK as specified in the IEEE802.15.4 standard. DSSS provides resistance to interference from other sources and efficient use of the available channels. IEEE 802.15.4 standard defines three bands of operation. In case of Wireless HART and ISA100.11a the wireless activity is confined to 2.4 GHz ISM band. Furthermore, a restriction on the use of Channel 26 is found in WirelessHART.[25]

C. Data link layer

ZigBee PRO has adopted the CSMA/CA access method of IEEE802.15.4, and for this reason does not guarantee deterministic communication. On the other hand, WirelessHART and ISA100.11a standards deviate from the CSMA/CA approach in the IEEE802.15.4 standard. They implement TDMA which provides deterministic time slots for the multiple transmitters in the network. The time slots in WirelessHART are fixed at 10 ms, whereas, they can be configured in ISA100.11 and WIA-PA. WirelessHART and ISA100.11a media access and network layers are based on Time Synchronized Mesh Protocol (TSMP) protocol originally designed by Dust Networks. TSMP is a reliable and scalable wireless networking protocol. In the case of WIA-PA the data link layer is based on IEEE 802.15.4 MAC. Other researchers considered some shortcomings the data link layer of WIA-PA in process control related to concurrent handling of real-time and nonreal-time messages. Channel hopping gives industrial protocols a high level of communication reliability. [13] ZigBee PRO supports frequency agility, which consists of scanning available channels to determine the channel with least interference, noise and traffic which is then selected and used by all ZigBee devices. Other protocols allow individual devices to choose different channels or different time slots for communication of individual packets. Poor quality channels may be blacklisted and taken out of use, and channels that have been found to provide good transmission can be whitelisted for preferential use. [10] Channel hopping also enhances network security because devices outside the network do not have information about the hopping sequence. The use of TDMA based MAC enables the design of a wireless network which is predictable. It is an important requirement for process automation and is achieved via TDMA because it allows accurate determination of latency. The operation of a TDMA based network requires time synchronization and a central NM. However, the use of a TDMA based centralized network approach limits a network size and its tolerance to varying network conditions.[20]

D. Network layer

The nodes in a wireless network are either Full Function Devices (FFDs) which can communicate with any other node, or Reduced Function Devices (FRDs) which can communicate only with an FFD. In general, FFDs do more communication and processing and hence consume more power. FFDs are needed to create a mesh network. The terminology is adopted from the ZigBee standard and is applied to the rest of the standards for a comparison. The top left panel shows a WirelessHART mesh network.[11]The gateway provides buffering of sensor data, diagnostics data and event notification. The field devices must be HART devices, either sensors or actuators configured in a mesh network. Mesh topology gives the network the capability of self-repair and self-optimization. All nodes are FFDs in the Wireless HART network. WirelessHART supports three modes of data routing, namely, graph routing, source routing and superframe routing as mentioned before. [16] The devices can be arranged in different topologies such as star or multi-hop mesh network. Some of the field devices are FFDs and may forward messages from other devices. The standard also allows the use of a high-speed network backbone (wired or wireless) for wide-area installation. ISA100.11a supports graph and source routing. ISA100.11a also supports IPv6 addressing WIA-PA network, comprises a hybrid topology with mobile handheld and field devices arranged in a star configuration around FFD nodes (cluster head) which are connected in a mesh. The network layer adopts static routing method for forwarding data packets. [22]

E. Gateway and NM

The wireless field network is managed by a NM which is responsible for setting up a network and supervising the network operations. It manages time slots, routing tables, schedules communications, monitors network health and queries field devices for information. In commercially available products, the gateway, NM and security manager are often housed in one system.[6]

F. Security

The security methods include: authentication which specifies which devices are allowed to join the network, encryption of data, and integrity checking which establishes that messages have not been tampered with.[14]

VI. CONCLUSION

This review has compared the standards and protocols suitable for use in wireless process automation. The aim has been to demonstrate why networks based on IEEE 802.15.4 are preferred and to support the discussions on research directions that follow in the rest of the paper. Additionally, a detailed investigation into the standards based on the IEEE 802.15.4 defined PHY are analyzed and it has been found that Wireless HART and ISA100.11a are well positioned to address the demands of process automation.

REFERENCES

1. Abouzeid, M.S., et al. Robust and low-complexity space time code for industrial automation. in 2018 10th International Conference on Advanced Infocomm Technology (ICAIT). 2018. IEEE.
2. Ikram, N. Thornhill, Wireless communication in process monitoring and control, Imperial College London, 2012.
3. Balog, M., M. Harris, and R. Buchert, Commissioning devices for automation systems. 2016, Google Patents.
4. Batalla, J.M., et al., On cohabitating networking technologies with common wireless access for home automation system purposes. IEEE Wireless Communications, 2016. **23**(5): p. 76-83.
5. Christin, D., P.S. Mogre, and M. Hollick, Survey on wireless sensor network technologies for industrial automation: The security and quality of service perspectives. Future Internet, 2010. **2**(2): p. 96-125.
6. Dewey, A.R., et al., Detection and location of wireless field devices. 2016, Google Patents.
7. Frotzscher, A., et al. Requirements and current solutions of wireless communication in industrial automation. in 2014 IEEE International Conference on Communications Workshops (ICC). 2014. IEEE.
8. Leitão, P., A.W. Colombo, and S. Karnouskos, Industrial automation based on cyber-physical systems technologies: Prototype implementations and challenges. Computers in Industry, 2016. **81**: p. 11-25.
9. Gunge, V.S. and P.S. Yalagi, Smart home automation: a literature review. International Journal of Computer Applications, 2016. **975**: p. 8887.
10. Li, J.-Q., et al., Industrial internet: A survey on the enabling technologies, applications, and challenges. IEEE Communications Surveys & Tutorials, 2017. **19**(3): p. 1504-1526.
11. Osseiran, A., J.F. Monserrat, and P. Marsch, 5G mobile and wireless communications technology. 2016: Cambridge University Press.
12. Jämsä-Jounela, S.-L., Future trends in process automation. Annual reviews in control, 2007. **31**(2): p. 211-220.
13. Mazur, D.C., S.D. Day, and B.K. Venne, Apparatus to interface process automation and electrical automation systems. 2019, Google Patents.
14. Patti, G., L. Leonardi, and L.L. Bello. A Bluetooth low energy real-time protocol for industrial wireless mesh networks. in IECON 2016-42nd Annual Conference of the IEEE Industrial Electronics Society. 2016. IEEE.
15. Gungor, V.C. and G.P. Hancke, Industrial wireless sensor networks: Challenges, design principles, and technical approaches. IEEE Transactions on industrial electronics, 2009. **56**(10): p. 4258-4265.
16. Pang, Z., M. Luvisotto, and D. Dzung, Wireless high-performance communications: The challenges and opportunities of a new target. IEEE Industrial Electronics Magazine, 2017. **11**(3): p. 20-25.
17. Zenuni, A., P. Reichert, and H. Schäuble, Housing lid for a field device of automation technology for wireless transmission of information. 2019, Google Patents.
18. Song, J., et al. WirelessHART: Applying wireless technology in real-time industrial process control. in 2008 IEEE Real-Time and Embedded Technology and Applications Symposium. 2008. IEEE.
19. Lu, C., et al., Real-time wireless sensor-actuator networks for industrial cyber-physical systems. Proceedings of the IEEE, 2015. **104**(5): p. 1013-1024.
20. Ehrlich, M., L. Wisniewski, and J. Jasperneite, State of the art and future applications of industrial wireless sensor networks, in Kommunikation und Bildverarbeitung in der Automation. 2018, Springer. p. 28-39.
21. Sha, M., et al. Implementation and experimentation of industrial wireless sensor-actuator network protocols. in European Conference on Wireless Sensor Networks. 2015. Springer.
22. Sha, M., et al., Empirical study and enhancements of industrial wireless sensor–actuator network protocols. IEEE Internet of Things Journal, 2017. **4**(3): p. 696-704.
23. Holfeld, B., et al., Wireless communication for factory automation: An opportunity for LTE and 5G systems. IEEE Communications Magazine, 2016. **54**(6): p. 36-43.
24. Gidlund, M., T. Lennvall, and J. Neander, Energy efficient method for communication between a wireless sensor network and an industrial control system. 2017, Google Patents.
25. Rentschler, M. Roaming in wireless factory automation networks. in 2017 22nd IEEE International Conference on Emerging Technologies and Factory Automation (ETFA). 2017. IEEE.

AUTHORS PROFILE

Nasr Rashid was born in Egypt, in 1973. He received the B.S. (with highest honors), M.S, and PhD in Electronics and Communication Engineering from Al-Azhar University, Cairo, Egypt in 1996, 2004, and 2009 respectively. He is currently an Assistant Professor in the Department of Electrical Engineering, College of Engineering, Jouf University, Sakaka, Saudi Arabia. His current research interests are in Wireless communications, Antennas, and Energy harvesting.

Osama I. Elhamrawy was born in Egypt, in 1976. He received the B.S., M.S, and PhD in Electronics and Communication Engineering from Al-Azhar University, Cairo, Egypt in 1999, 2006, and 2011 respectively. He is currently an Assistant Professor in the Department of Electrical Engineering, College of Engineering, Jouf University, Sakaka, Saudi Arabia. His current research interests are in Electronics, Multilevel Inverters, and Wireless Communications.